Computer Architecture

TECHNICAL REPORT

NYU COMPSCI TR-156 c.1
CANTONE Decisions
procedures for...

RESEARCH REPORT
CANTONE
DECISIONS
PROCEDURES FOR...

Author
Title

Abstract

TECHNICAL REPORT

1

DECISION PROCEDURES FOR ELEMENTARY SUB-
LANGUAGES OF SET THEORY. VI. MULTI-LEVEL
SYLLOGISTIC EXTENDED BY THE POWERSET
OPERATOR.

By

D. Cantone
A. Ferro
J.T. Schwartz

February 1985
Technical Report #156

DECISION PROCEDURES FOR ELEMENTARY SUBLANGUAGES OF SET THEORY.

VI. MULTI-LEVEL SYLLOGISTIC EXTENDED BY THE POWERSSET OPERATOR.

D. Cantone, A. Ferro and J. T. Schwartz

Computer Science Department, Courant Institute of Mathematical Sciences
New York University

and

Mathematics Department, University of Catania, Italy

1. INTRODUCTION.

In this paper we show that the unquantified theory of sets in the language $\emptyset$ (empty set), $=$ (equality), $\in$ (membership), $\cup$ (union), $\setminus$ (set difference) and pow (powerset) is decidable. The more restricted theory obtained by dropping the powerset operator was considered in [FOS 80]. The case in which at most two occurrences of the powerset operator are allowed was solved in [BF 84]. We use techniques and ideas recently developed in [CFS 84], [F 84], and [CFMS 84].

2. PRELIMINARIES.

We consider the theory MLS [see FOS 80] which is the set of formulas built using the Boolean connectives (conjunction, disjunction, implication and negation) from set theoretic atoms of the following types:

$$(2.1) \quad x = y \cup z, \quad x = y \setminus z, \quad x \in y, \quad x = \emptyset.$$

In [FOS 80] an algorithm which decides satisfiability of any formula P of MLS is described. We summarize the method in the following way. We can assume without loss of generality that P is simply a conjunction of clauses of types (2.1) and clauses of the form $x \neq y$.

Definition 2.1. A place α of P is a 0/1-valued function defined on the set of all variables in P such that $\alpha(x) = \alpha(y) \vee \alpha(z)$ (resp. $\alpha(x) = \alpha(y) \wedge \alpha(z)$) if $x = y \cup z$ (resp. $x = y \cap z$), belongs to P , and such that $\alpha(x) = 0$ if $x = \emptyset$ appears in P . Given a variable x , the place α is said to be a place of P at x if $\alpha(y) = 1$ (resp. $\alpha(y) = 0$) whenever $x \in y$ (resp. $x \notin y$) appears in P .

The set Π of all possible places of P is finite and easily calculated. On the other hand any model M of P defines a set Π_M of places of P in the following way. Let p be any element of some M_x for some variable x in P ; then the function defined by

$$(2.2) \quad \alpha(y) = \begin{cases} 1 & \text{if } p \in M_y \\ 0 & \text{if } p \notin M_y \end{cases}$$

is clearly a place, and for each variable z we obtain a place α_z which is a place at z , by taking $p = M_z$. Notice also that the places of Π_M can equivalently be defined as those places α of p for which the set

$$(2.3) \quad \sigma_\alpha = \{p \mid p \in M_x \Leftrightarrow \alpha(x) = 1 \text{ for all variables } x\}$$

is nonempty. We observe that the following properties hold:

$$(2.4) \quad M_x = \bigcup_{\alpha(x)=1} \sigma_\alpha \text{ for each variable } x;$$

(2.5) the sets σ_α are nonempty and pairwise disjoint.

Moreover with each variable x there is associated a place α_x such that:

$$(2.6) \quad Mx \in \sigma_{\alpha_x}.$$

We note also that two variables x, y are such that $Mx = My$ if and only if $\alpha(x) = \alpha(y)$ for every $\alpha \in \Pi_M$. We express this fact by saying that x and y are Π_M -equivalent.

Finally, we observe that the variables can be ordered in such a way that

$$(2.7) \quad \alpha_x(y) = 1 \Rightarrow x < y.$$

The converse is established by the following theorem [FOS 80].

Theorem 2.2. If there exists a set Π of places of P such that after identification of Π -equivalent variables it is possible to associate a place $\alpha_x \in \Pi$ at x for each x and to order variables in such a way that condition (2.7) is satisfied then P has a model. Moreover a model M of P can be defined by (2.4) provided that sets σ_α satisfying (2.5) and (2.6) have been chosen.

3. THE MAIN RESULT.

We will present an algorithm which decides satisfiability of any conjunction P of clauses of types (2.1), plus clauses of the form $x \neq y$, plus additional clauses of the following form:

$$(3.1) \quad p_i = \text{pow}(q_i), \quad i = 1, 2, \dots, k.$$

It proves convenient to assume also, without loss of generality, that clauses

$$(3.2) \quad q_0 = \emptyset \quad \& \quad p_0 = \text{pow}(q_0) \quad \& \quad q_0 \in p_0$$

are present in Q . Note that in the presence of these clauses it follows that $\sigma_{\alpha_\emptyset} = \{\emptyset\}$ (for any model M of all our clauses, and for σ_α defined by (2.3)), where by $\alpha_\emptyset$ we designate the place α_{q_0} .

To begin the analysis necessary to justify the algorithm to be presented, let Π be a set of places of (the MLS sentences of) P , and assume that variables which are necessarily Π -equivalent in consequence of the clauses of P other than those of powerset form have been identified.

Definition 3.1. (a) For any sets $s_1, \dots, s_m$ let $\text{pow}^*(s_1, \dots, s_m)$ denote the collection of all nonnull elements of $\text{pow}(s_1 \cup \dots \cup s_m)$ which have non-null intersections with every one of the sets s_j .

(b) A non-empty set $\{\alpha_1, \dots, \alpha_l\}$ of places is called a P-node if there is a powerset clause $p_i = \text{pow}(q_i)$ such that $\alpha_j(q_i) = 1$ for all $j = 1, \dots, l$.

(c) Let A be a P-node. A place β is called a target of A if for every powerset clause $p_i = \text{pow}(q_i)$ we have $\beta(p_i) = 1$ if and only if $\alpha(q_i) = 1$ for all $\alpha \in A$, in which case we write $A \rightarrow \beta$, and call the relationship $A \rightarrow \beta$ a P-edge.

(d) A place β is called initial if it is not the target of any P-node A.

The following very simple lemma follows easily from Definition 3.1a above.

Lemma 3.2. If $s_1, \dots, s_\ell$ and $t_1, \dots, t_m$ is a collection of nonempty sets which are pairwise disjoint if not identical then

$$\text{pow}^*(s_1, \dots, s_\ell) \cap \text{pow}^*(t_1, \dots, t_m) \neq \emptyset \Leftrightarrow \{s_1, \dots, s_\ell\} = \{t_1, \dots, t_m\}.$$

Remark. Note, in clarification of the argument which follows, that if a model M of P exists and $\{\alpha_1, \dots, \alpha_\ell\}$ is a P-node, then the 'syntactic' relationship $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \beta$ is implied by the 'semantic' relationship $\text{pow}^*(\sigma_{\alpha_1}, \dots, \sigma_{\alpha_\ell}) \cap \sigma_\beta \neq \emptyset$. Indeed, let $s \in \text{pow}^*(\sigma_{\alpha_1}, \dots, \sigma_{\alpha_\ell}) \cap \sigma_\beta$. Then $s = \bigcup_{1 \leq i \leq \ell} (s \cap \sigma_{\alpha_i})$, and all the terms in this union are non-null. Moreover for all powerset clauses $p_j = \text{pow}(q_j)$ we have

$$\begin{aligned} \beta(p_j) = 1 &\Leftrightarrow s \in Mp_j \Leftrightarrow s \in \text{pow}(Mq_j) \\ &\Leftrightarrow s \cap \sigma_{\alpha_i} \subseteq Mq_j \text{ for all } i = 1, \dots, \ell \\ &\Leftrightarrow \alpha_i(q_j) = 1 \text{ for all } i = 1, \dots, \ell, \end{aligned}$$

implying $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \beta$.

The reader will find the course of the argument which follows

clearer if the fact that $\{\alpha_1, \dots, \alpha_l\} \rightarrow \beta$ is intended as a syntactic representation for the underlying semantic relationship $\text{pow}^*(\sigma_{\alpha_1}, \dots, \sigma_{\alpha_l}) \cap \sigma_{\beta} \neq \emptyset$ is borne in mind.

Let M be a model of P and let $\Pi = \Pi_M$ be the set of places associated with M in the manner described in the preceding section. We shall show that the six decidable conditions given below all hold, and conversely we shall show all that these conditions imply the existence of a map $\alpha \mapsto \bar{\alpha}$ from places to non-empty sets such that the assignment defined by $x \mapsto \bigcup_{\alpha(x)=1} \bar{\alpha}$, models all conjuncts in P of type $x = y \cup z$, $x = y \setminus z$, $x = \emptyset$, and $x \neq y$. However, this assignment will only satisfy 'approximate' powerset clauses; more specifically, it will satisfy $\bigcup_{\alpha(p_i)=1} \bar{\alpha} \subseteq \text{pow}(\bigcup_{\alpha(q_i)=1} \bar{\alpha})$ for any clause $p_i = \text{pow}(q_i)$ in P . However once this point is reached it will follow that the sets $\bar{\alpha}$ can be enlarged in such a way as to satisfy the powerset and membership clauses, also i.e. those of type $x \in y$ and $p = \text{pow}(q)$. This will show that a model of P can be constructed, thus proving the decidable conditions that we now proceed to list are necessary and sufficient for satisfiability.

CONDITION C1. For every variable x there exists an $\alpha_x \in \Pi$ which is a place of P at x , so that $\alpha_x(y) = 1$, (resp. $\alpha_x(y) = 0$) if the clause $x \in y$ (resp. $x \notin y$) appears in P .

CONDITION C2. There is an ordering of variables such that q_0 is the minimum variable and such that

$$\alpha_x(y) = 1 \Rightarrow x < y.$$

CONDITION C3. The place α_{q_0} , which we also denote as $\alpha_\emptyset$, is an initial place.

CONDITION C4. For every variable x and every $j = 0, 1, \dots, k$ we have

$$\alpha_x(p_j) = 1 \Leftrightarrow (\forall \alpha \in \Pi) [\alpha(x) = 1 \Rightarrow \alpha(q_j) = 1] .$$

CONDITION C5. The P-edges $A \rightarrow \alpha$ can be marked in such a way that:

- (a) for every P-node $A = \{\alpha_1, \dots, \alpha_\ell\}$ there is one and only one marked edge $A \rightarrow \alpha$. (If the edge $A \rightarrow \alpha$ is marked α will be called the principal target of A .)
- (b) Let x be any variable appearing in P . If $\{\alpha_1, \dots, \alpha_\ell\} = \{\beta \in \Pi \mid \beta(x) = 1\}$ is a P-node then there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha_x$, and this edge is marked.
- (c) There is an ordering $\prec^*$ of places such that
 - (c1) If the P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ is marked then $\alpha_1 \prec^* \alpha$ for all $i = 1, \dots, \ell$.
 - (c2) $y \preceq x$ & $\alpha_x \prec^* \beta \Rightarrow \beta(y) = 0$.

CONDITION C6. It is possible to define a mapping $\alpha \mapsto \bar{\alpha}$ from the places $\alpha \in \Pi$ to sets $\bar{\alpha}$ satisfying the following conditions:

- (a) Each $\bar{\alpha}$ is a finite nonempty set and every element of $\bar{\alpha}$ either has a finite rank or a rank which exceeds ω , where ω designates the first infinite ordinal (ω is equivalent to the set $\{0, 1, \dots\}$ of all integers).
- (b) $\bar{\alpha} \cap \bar{\beta} = \emptyset$ if $\alpha \neq \beta$.
- (c) $\bigcup_{\alpha(p_j)=1} \bar{\alpha} \subseteq \text{pow}(\bigcup_{\beta(q_j)=1} \bar{\beta})$ for every clause of the form $p_j = \text{pow}(q_j)$.

- (d) If $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \cap \bar{\alpha} \neq \emptyset$ then there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$.
- (e) If $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell \in \bar{\alpha}$ then the P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ is marked.
- (f) If s is a non-empty set of rank different from $\omega+1$ such that $s \in \bar{\alpha}$ for some place α , then there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ such that $s \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$.

Moreover, it must be possible to produce these sets by executing the following nondeterministic Initialization Algorithm, and, indeed, by executing STEP 2 of the algorithm at most $n2^{n\rho}$ times in some appropriate sequence, where n is the number of places in Π and ρ is any integer such that $2^{\rho-1}/n \geq \rho$.

Initialization Algorithm

STEP 1. Let $\alpha_0, \beta_1, \dots, \beta_r$ be the initial places of G and for $i, j = 1, 2, \dots$ let λ_{ij} designate pairwise distinct doubleton sets of the form $\{r, \omega\}$, where r is a positive integer and $\omega \in \{0, 1, 2, \dots\}$ is the infinite collection of all integers. (We shall call such sets λ_{ij} individuals.) Put

$$\bar{\alpha}_0 = \{\emptyset\};$$

$$\bar{\beta}_i = \{\lambda_{i1}, \lambda_{i2}, \dots, \lambda_{i\rho}\}, \quad i = 1, 2, \dots, r;$$

$$\bar{\alpha} = \emptyset \quad \text{for every } \alpha \in \Pi, \alpha \text{ not initial};$$

(where ρ is any integer such that $2^{\rho-1}/n \geq \rho$).

STEP 2. Pick a P-node $A = \{\alpha_1, \dots, \alpha_\ell\}$ and let $\gamma_1, \dots, \gamma_m$ be the places

for which there exists a P-edge $A \rightarrow \gamma_i$. Let $t_1, t_2, \dots, t_m$ be sets such that

$$t_i \subseteq [\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_l)] \setminus \bigcup_{A \rightarrow \alpha} \bar{\alpha}$$

for all $i = 1, \dots, m$, and enlarge $\bar{\gamma}_i$ by putting $\bar{\gamma}_i + \bar{\gamma}_i \cup t_i$.

GOTO STEP 2 OR STOP.

Remark 1. Note that as the algorithm executes, the sets $\bar{\alpha}$ increase steadily.

Remark 2. Notice that since the sets $\bar{\alpha}$ which can arise at each step of the Initialization Algorithm are finite it follows that condition (C6) is decidable. If we did not impose the condition that the sets appearing in (C6-a) through (C6-e) were produced by an a priori limited number of steps by the above Initialization Algorithm, this would no longer be the case.

As usual we will proceed by showing that satisfiability of the family of clauses defining P implies existence of a family of sets, orderings, etc. satisfying (C1)-(C6), and then conversely show that if (C1)-(C6) are satisfied then P has a model. That (C1)-(C5) are necessary for satisfiability is easy to see, and we treat this point first. Then, postponing discussion of the somewhat more intricate point (C6), we will prove that (C1)-(C6) are sufficient for satisfiability. Finally, we will return to a discussion of (C6), and prove that, like (C1)-(C5), it is necessary for satisfiability.

To see that (C1)-(C5) are necessary, again let M be a model of our set of clauses, define the set $\Pi = \Pi_M$ of all places of M as in the

paragraph preceding (2.2), define the sets σ_α by (2.3), and define the place α_y at a variable y by (2.2). Then conditions (C1)-(C5) can be proved as follows:

Proof of (C1) and (C2): Conditions (C1) and (C2) follow just as in the simple MLS case described in the preceding section. The ordering of variables appearing in condition (C2) can be any linear ordering extending the acyclic relationship $x < y \leftrightarrow \text{rank}(Mx) < \text{rank}(My)$.

Proof of (C3): Since $\alpha_\emptyset(p_0) = 1$, then if $\{\alpha_1, \dots, \alpha_l\} \rightarrow \alpha_\emptyset$ it follows that $\alpha_i(q_0) = 1$ for every $i = 1, \dots, l$. This is impossible by (3.2), since $Mq_0 = \emptyset$. It follows that $\alpha_\emptyset$ is initial.

Proof of (C4): Let x be a variable and $p_j = \text{pow}(q_j)$ a powerset clause in P . Then by (2.2) $\alpha_x(p_j) = 1 \Leftrightarrow Mx \in Mp_j \Leftrightarrow Mx \in \text{pow}(Mq_j) \Leftrightarrow Mx \subseteq Mq_j \Leftrightarrow \sigma_\alpha \subseteq Mq_j$ for all $\sigma_\alpha \subseteq Mx \Leftrightarrow \alpha(q_j) = 1$ for all α such that $\alpha(x) = 1$.

Proof of (C5): We define a marking of P -edges by marking a P -edge $\{\alpha_1, \dots, \alpha_l\} \rightarrow \alpha$ if and only if $\sigma_{\alpha_1} \cup \dots \cup \sigma_{\alpha_l} \in \sigma_\alpha$ (where σ_α is defined by (2.3)). Moreover we order variables and places by any ordering extending the order of ranks of the sets Mx and σ_α respectively. Let x be a variable and let $\{\beta_1, \dots, \beta_m\}$ be the set of all places β such that $\beta(x) = 1$, so that $Mx = \bigcup_{1 \leq i \leq m} \sigma_{\beta_i}$. Let $p_j = \text{pow}(q_j)$ be any one of the powerset clauses in the set P . Then

$$\begin{aligned} \alpha_x(p_j) = 1 &\Leftrightarrow Mx \in Mp_j \Leftrightarrow Mx \subseteq Mq_j \Leftrightarrow \sigma_{\beta_i} \subseteq Mq_j \text{ for all } 1 \leq i \leq m \\ &\Leftrightarrow \beta_i(q_j) = 1 \text{ for all } 1 \leq i \leq m, \end{aligned}$$

proving that if $\{\beta_1, \dots, \beta_m\}$ is a P -node then there exists a P -edge

$\{\beta_1, \dots, \beta_m\} \rightarrow \alpha_x$. It is also plain that with the specified choice of marking and ordering, condition (C5c) is satisfied.

We postpone discussion of (C6) to the next section, and go on immediately to show that satisfiability of (C1)-(C6) is sufficient for satisfiability of the initially given set P of clauses.

To this end, assume first of all that a set Π of places of P has been found and that all variables which are Π -equivalent in virtue of the non-powerset clauses of P have been identified. Assume also that an ordering $<$ of variables and an ordering $\prec^*$ of places exist in such a way that conditions (C1)-(C6) are satisfied where P-edges are defined by Definition 3.1. Let $\{\bar{\alpha} \mid \alpha \in \Pi\}$ be a collection of sets satisfying conditions (C6a,b,c,d,e). Notice that if we put

$$(3.3) \quad Mx = \bigcup_{\alpha(x)=1} \bar{\alpha}$$

for every variable x then M defines a model of all literals of P not involving clauses of the form $x \in y$ or $p = \text{pow}(q)$. In order to satisfy these additional literals, we apply the following 'filling' algorithm, whose steps (a) and (b) force the model M to satisfy the ϵ - and pow-clauses respectively.

"Filling" Algorithm

STEP (a) Process successive variables x in the ordering " $<$ " of variables by putting

$$M_x = \bigcup_{\alpha(x)=1} \bar{\alpha} ;$$

and setting

$$\bar{\alpha}_x + \bar{\alpha}_x \cup \{M_x\} .$$

As soon as the variable x has been processed apply the following

STEP (b). For successive places $\alpha \succ^* \alpha_x$ in the ordering $\prec^*$ of places α do:

If $A = \{\alpha_1, \dots, \alpha_l\} \rightarrow \alpha$ is marked then put

$$\bar{\alpha} + \bar{\alpha} \cup [\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_l) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}]$$

IF unprocessed variables remain, go to Step (a);

otherwise STOP.

Note that step (b) modifies only sets $\bar{\alpha}$ for which $\alpha \succ^* \alpha_x$ after $\bar{\alpha}_x$ has been modified by step (a).

LEMMA 3.3. The following properties hold at every step of the Filling Algorithm.

(3.4) Every $\bar{\alpha}$ is nonempty, finite and every element $t \in \bar{\alpha}$

has a rank which is either finite or which is greater than ω .

(3.5) $\bar{\alpha} \cap \bar{\beta} = \emptyset$ whenever $\alpha \neq \beta$.

(3.6) $\bigcup_{\alpha(p_j)=1} \bar{\alpha} \subseteq \text{pow}(\bigcup_{\beta(q_j)=1} \bar{\beta})$

for every clause of the form $p_j = \text{pow}(q_j)$.

(3.7) If $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \cap \bar{\alpha} \neq \emptyset$ and $\{\alpha_1, \dots, \alpha_\ell\}$ is a P-node, then there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$.

(3.8) (i) We have $Mx \in \bar{\alpha}_x$ for every variable x which has been processed in step (a).

(ii) For each variable x let $\beta_1, \dots, \beta_m$ be all the places β such that $\beta(x) = 1$. Then

$$\bar{\beta}_1 \cup \dots \cup \bar{\beta}_m \in \bar{\alpha} \Rightarrow \alpha = \alpha_x.$$

Proof: We proceed by induction on the number of steps executed. When the Filling Algorithm starts, conditions (3.4)-(3.7) hold by (C6a,b,c,d) respectively. Condition (3.8i) is vacuously satisfied since no variable has been processed yet. Condition (3.8ii) follows by (C6e) and (C5a,C5b).

Next we assume that conditions (3.4)-(3.8) hold up to execution of a step S of the Filling Algorithm and will show that they continue to hold after S is executed.

Proof of (3.4): Notice that any single step S of the Filling Algorithm modifies a set $\bar{\alpha}$ by adding to it either a singleton or a finite subset of $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$ for some places $\alpha_1, \dots, \alpha_\ell$. It follows by induction that $\bar{\alpha}$ will remain nonempty and finite after S is executed. Moreover by induction every element added to $\bar{\alpha}$ has a rank which is either finite or which is greater than ω .

Proof of (3.5): We distinguish two cases:

Case (1): Assume that step S is step (a), performed relative to a variable x . It follows by the induction hypothesis (3.8ii)

that if $Mx \in \bar{\alpha}$ before step S is executed then $\alpha = \alpha_x$. This shows that disjointness of the sets $\bar{\alpha}$ cannot be destroyed by executing such a step S.

Case (2): Assume that step S is a 'stabilization' step (b) relative to a marked P-edge $A = \{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$. Then step S performs the operation

$$\bar{\alpha} \leftarrow \bar{\alpha} \cup [\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}].$$

If disjointness were disrupted by step S, then for some place γ we would have $\bar{\alpha} \cap \bar{\gamma} \neq \emptyset$. But before step S is executed $\bar{\alpha} \cap \bar{\gamma} = \emptyset$, so that

$$(3.9) \quad [\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}] \cap \bar{\gamma} \neq \emptyset$$

must have been true at that time. Hence by the induction hypothesis (3.7) $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \gamma$ must be a P-edge, implying that $\bar{\gamma} \subseteq \bigcup_{A \rightarrow \beta} \bar{\beta}$, which contradicts (3.9).

Proof of (3.6): Again we distinguish two cases:

Case (1): Let step S be step (a) relative to a variable x . If $\alpha_x(p_j) = 1$ then it follows by condition (C4) that $\alpha(x) = 1 \Rightarrow \alpha(q_j) = 1$ for every place α in Π . This implies that $Mx \in \text{pow}(\bigcup_{\beta(q_j)=1} \bar{\beta})$, showing that property (3.6) cannot be spoiled by such a step S.

Case (2): Let step S be a stabilization step (b) relative to a marked P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$. If $\alpha(p_j) = 1$ then it follows by Definition 3.1 that $\{\alpha_1, \dots, \alpha_\ell\} \subseteq \{\beta \mid \beta(q_j) = 1\}$. Therefore

only elements of $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \subseteq \text{pow}(\bigcup_{\beta(q_j)=1} \bar{\beta})$ are added to $\bar{\alpha}$ by step S, showing that (3.6) still holds after execution of such a step.

Proof of (3.7): Let $\{\alpha_1, \dots, \alpha_\ell\}$ be a P-node, and let $\bar{\alpha} \cap \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \neq \emptyset$ just after step S is executed. Suppose first that $s \in \bar{\alpha} \cap \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$ is an element newly introduced into $\bar{\alpha}$ by step S, and that S is a step (a) relative to some variable x , so that $s = \bar{\beta}_1 \cup \dots \cup \bar{\beta}_m \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m)$, where $\{\beta_1, \dots, \beta_m\}$ is the set of all places β such that $\beta(x) = 1$; moreover, by (3.5) we have $\alpha = \alpha_x$. It follows by (3.5) and Lemma 3.2 that $\{\alpha_1, \dots, \alpha_\ell\} = \{\beta_1, \dots, \beta_m\}$. Therefore $\{\beta_1, \dots, \beta_m\}$ is a P-node and by (C5b) $\{\beta_1, \dots, \beta_m\} \rightarrow \alpha_x = \alpha$ is a (marked) P-edge, and hence there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ also.

If on the other hand s is newly introduced into $\bar{\alpha}$ by a step S of type (b), then by definition of steps of this kind (see the Filling Algorithm) there exists a P-edge $\{\beta_1, \dots, \beta_m\} \rightarrow \alpha$ such that $s \in \text{pow}^*(\beta_1, \dots, \beta_m)$. Again we have $\{\beta_1, \dots, \beta_m\} = \{\alpha_1, \dots, \alpha_\ell\}$ by (3.5) and Lemma 3.2, so that again there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$.

Next suppose that $s \in \bar{\alpha} \cap \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$ is not introduced into $\bar{\alpha}$ by step S. Since $s \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \subseteq \text{pow}(\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell)$, elements of s are also elements of some $\bar{\alpha}_j$, and hence by (3.4) s is either of finite rank, or has an element of rank greater than ω , i.e. s has rank greater than $\omega+1$. Since $s \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$, s has a non-null intersection with every set $\bar{\alpha}_j$, and therefore $s \neq \emptyset$. By these last two assertions and (C6f) it follows that if s is present in $\bar{\alpha}$ even before the Filling Algorithm starts, then there exists a P-edge $\{\beta_1, \dots, \beta_m\} \rightarrow \alpha$ such that $s \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m)$. The same conclusion

holds even in the case in which s is introduced into $\bar{\alpha}$ by an earlier type (b) step S_0 of the Filling Algorithm. In both these cases it further follows by (3.5) and Lemma 3.2 that $\{\alpha_1, \dots, \alpha_k\} = \{\beta_1, \dots, \beta_m\}$ which proves that $\{\alpha_1, \dots, \alpha_k\} \rightarrow \alpha$ is a P-edge.

It only remains to consider the case in which s was added to $\bar{\alpha}$ by an earlier type (a) step S_0 involving a variable x . In this case, $s = \bar{\beta}_1 \cup \dots \cup \bar{\beta}_m$, where $\{\beta_1, \dots, \beta_m\}$ is the set of all β such that $\beta(x) = 1$, and moreover $\alpha = \alpha_x$. By (3.5) and Lemma 3.2 $\{\beta_1, \dots, \beta_m\} = \{\alpha_1, \dots, \alpha_k\}$, so that $\{\beta_1, \dots, \beta_m\}$ is a P-node. Therefore by (C5b) $\{\beta_1, \dots, \beta_m\} \rightarrow \alpha_x = \alpha$ is a P-edge, i.e. $\{\alpha_1, \dots, \alpha_k\} \rightarrow \alpha$ is a P-edge, completing the proof of (3.7).

Proof of (3.8i):

Case (1): If the step S is a stabilization step (b) then it will only modify places $\bar{\beta}$ such that $\bar{\beta} \not\geq \alpha_x$, where x is the variable most recently processed in step (a). By (C5c2) modification of $\bar{\beta}$ for such a place β causes no change in any M_y for any previously processed variable y . Thus no previously established assertion $M_y \in \bar{\alpha}_y$ loses its validity.

Case (2): If S is a step of type (a) relative to a variable x , then immediately after step S the variables y that have been processed are exactly those for which $y \leq x$. But for all such variables y except x itself, $\alpha_x(y) = 0$ by condition (C2). Hence $M_y \in \bar{\alpha}_y$ remains true for every $y < x$, while plainly $M_x \in \bar{\alpha}_x$ just after step S .

Proof of (3.8ii): Let $\{\beta_1, \dots, \beta_m\}$ be the set of all places β such that

$\beta(x) = 1$. Suppose that immediately after execution of step S we have

$$\bar{\beta}_1 \cup \dots \cup \bar{\beta}_m \in \bar{\alpha}$$

Case (1): Assume that $\bar{\beta}_1 \cup \dots \cup \bar{\beta}_m$ was put into $\bar{\alpha}$ by step S.

We distinguish two subcases.

Case (1a). Let S be a step of type (a) relative to a variable z.

Then $Mz = \bar{\beta}_1 \cup \dots \cup \bar{\beta}_m$ and $\alpha = \alpha_z$. It follows by (3.4) and (3.5) that for each place $\beta \in \Pi$ $\beta(z) = \beta(x)$, from which $x = z$ and $\alpha = \alpha_x$ follow immediately.

Case (1b). Next let S be a stabilization step determined by a marked P-edge

$$A = \{\alpha_1, \dots, \alpha_2\} \rightarrow \alpha.$$

Then (see the definition of the Filling Algorithm)

$$\bar{\beta}_1 \cup \dots \cup \bar{\beta}_m \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_2), \quad \text{and} \quad \text{since} \\ \bar{\beta}_1 \cup \dots \cup \bar{\beta}_m \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \text{ it follows by (3.5) and}$$

Lemma 3.2 that $\{\alpha_1, \dots, \alpha_2\} = \{\beta_1, \dots, \beta_m\}$. The P-edge $\{\beta_1, \dots, \beta_m\} \rightarrow \alpha$ is therefore marked, which implies $\alpha = \alpha_x$ by condition (C5a,b).

Case (2): Assume that the new value of $\bar{\beta}_1 \cup \dots \cup \bar{\beta}_m$ belonged to $\bar{\alpha}$ before the last step S was executed. If $\bar{\beta}_1 \cup \dots \cup \bar{\beta}_m$ is not modified by step S then $\alpha = \alpha_x$ by induction hypothesis. The only other possibility contradicting our assertion is that some new element t should have been put in some $\bar{\beta}_i$ by the step S, and that the new value $s = \bar{\beta}_1 \cup \dots \cup \bar{\beta}_m$ thereby produced should have been a member of $\bar{\alpha}$ before the step S. In this case it follows by (C6a) that $s \neq \emptyset$ and that the rank of s is different from $\omega+1$. Hence, if s was in $\bar{\alpha}$ even before

the Filling Procedure started, it follows by (C6f) that there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ such that $s \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$. Moreover, the same conclusion applies (by definition of the Filling Algorithm) if s was introduced into $\bar{\alpha}$ by an earlier type (b) step S_0 . On the other hand if s was introduced into $\bar{\alpha}$ by an earlier type (a) step S_0 relative to a variable z , then $s = \bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell$, where $\alpha_1, \dots, \alpha_\ell$ are all the places α such that $\alpha(z) = 1$, so that $s \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$ in this case also. Hence in every case we must have $s \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$ for some places $\alpha_1, \dots, \alpha_\ell$ (where $\bar{\alpha}_1, \dots, \bar{\alpha}_\ell$ are to be understood as the values assumed by the indicated sets at some time before step S was executed). Since $s \subseteq \bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell$, it follows that t must have been an element of some $\bar{\alpha}_j$ even before step S was executed, which by (3.5) contradicts the fact that t is introduced for the first time into $\bar{\beta}_1$ by step S .

This completes the proof of Lemma 3.3.

It is now easy to finish the first part of the proof that conditions (C1)-(C6) are sufficient for satisfiability of the set P of clauses. Plainly, when execution of the Filling Algorithm terminates conditions (C1), (3.4), (3.5) and (3.8i) imply that (3.3) will define a model M of all literals of P except possibly the power set literals of the form $p_i = \text{pow}(q_i)$. To see that these literals are correctly modeled also we argue as follows. By (3.6) we have

$$(3.10) \quad Mp_j = \bigcup_{\alpha(p_j)=1} \bar{\alpha} \subseteq \text{pow} \left(\bigcup_{\beta(q_j)=1} \bar{\beta} \right) = \text{pow}(Mq_j)$$

for all powerset clauses $p_j = \text{pow}(q_j)$ in P . On the other hand let $s \in \text{pow}(Mq_j)$ (where $0 < j \leq k$). If $s = \emptyset$ then by (C4) we have $s \in \bar{\alpha}\emptyset \subseteq Mp_j$. Otherwise, if $s \neq \emptyset$, let $\beta_1, \dots, \beta_m$ be all the places β for which $s \cap \bar{\beta} \neq \emptyset$. Since $s \subseteq Mq_j$, we have $\beta_i(q_j) = 1$, for all $i = 1, \dots, m$ by (3.3) and (3.5). Therefore $B = \{\beta_1, \dots, \beta_m\}$ is a P-node. Let α be the principal target of $\{\beta_1, \dots, \beta_m\}$ (the existence of α is assured by condition (C5a); see also note to (C5b)). Consider the last time that a step (b) of the Filling Algorithm is executed relative to the marked P-edge $\{\beta_1, \dots, \beta_m\} \rightarrow \alpha$. By the ordering condition (C5cl) no set $\bar{\beta}_1, \dots, \bar{\beta}_m$ changes any more after this last assignment, which has the form

$$\bar{\alpha} + \bar{\alpha} \cup [\text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \setminus \bigcup_{B \rightarrow \gamma} \bar{\gamma}] .$$

Moreover, since $s \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m)$ the statement $s \in \bigcup_{B \rightarrow \gamma} \bar{\gamma}$ must hold after this assignment is performed. Since $\beta_i(q_j) = 1$ for all $\beta_i \in B$, it follows by definition (3.1b) of P-edges that $\gamma(p_j) = 1$ for every target γ of B , which implies that $\bigcup_{B \rightarrow \gamma} \bar{\gamma} \subseteq Mp_j$. Thus $s \in Mp_j$, i.e. $Mp_j \subseteq \text{pow}(Mq_j)$ for every $j = 0, \dots, k$, which together with (3.10) shows that $Mp_j = \text{pow}(Mq_j)$, for every $j = 0, \dots, k$.

The argument just given makes it plain that the proof of our main decidability result will be complete as soon as point (C6) above has been treated adequately. We now return to discuss this issue.

4. PROOF OF NECESSITY OF CONDITION (C6).

To prove condition (C6) we use the existence of a model M to instantiate the nondeterministic Initialization Algorithm which appears in this section. In this instantiation, which is shown just below, the notation $|s|$ designates the cardinality of the set s . The algorithm makes use of the sets σ_α defined by (2.3).

Instantiated Variant of the Initialization Algorithm

Begin by defining $\bar{\alpha}$ for every initial place α as in STEP 1 of the Initialization Algorithm described in condition (C6) of the preceding section. Then repeat the following loop:

WHILE there exists at least one place α such that $|\bar{\alpha}| < \rho$ and

$\bar{\alpha} \neq \sigma_\alpha$ DO:

IF there is at least one P-node $A = \{\alpha_1, \dots, \alpha_\ell\}$ and P-edge $A \rightarrow$

α such that $|\alpha| < \rho$, $\bar{\alpha} \neq \sigma_\alpha$, $\bar{\alpha}_j \neq \emptyset$ for $j = 1, \dots, \ell$, and

some $\bar{\alpha}_j$, $j = 1, \dots, \ell$, satisfies $|\bar{\alpha}_j| \geq \rho$, DO:

Step (a): Pick pairwise disjoint sets $t_\alpha \subseteq \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}$,

one for each α such that $A \rightarrow \alpha$, in such a way that

(a1) $|t_\alpha| \geq \rho$ for every such α

(a2) The set $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell$ must belong to t_α , where α is the unique (see (C5a)) principal target of A .

Put $\bar{\alpha} \leftarrow \bar{\alpha} \cup t_\alpha$ for each such α ;

[Comment: We will show below that sets t_α having the stated properties

exist whenever Step (a) is executed. Indeed, by clause (4.7) of

Lemma 4.1 below, we have $|\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}| \geq \rho \cdot n$.

Therefore, considering that the P-node A can have at most n

targets, it follows that the number of elements in $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_2) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}$ is large enough to satisfy (a1) above. Condition (4.7) of Lemma 4.1 implies that $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_2 \notin \bigcup_{A \rightarrow \beta} \bar{\beta}$, so that the element $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_2$, which clearly belongs to $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_2)$ can be put in t_α , where α is the principal target of A , so that (a2) can also be satisfied.]

ELSE

Step (b). Pick any P-edge $A = \{\alpha_1, \dots, \alpha_2\} \rightarrow \alpha$ such that

$$|\bar{\alpha}| < \rho, \bar{\alpha} \neq \sigma_\alpha, \text{ and}$$

$$\Delta_A = (\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_2) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}) \neq \emptyset.$$

For each β such that $A \rightarrow \beta$, put $\bar{\beta} + \bar{\beta} \cup (\Delta_A \cap \sigma_\beta)$.

[Comment: We will show below that such a P-edge $A \rightarrow \alpha$ can be selected whenever this branch of the IF is reached; this is clause (4.8) of Lemma 4.1.]

END IF;

END WHILE;

Remark 1. Note that the foregoing, which assumes the existence of a model, is indeed an instantiation of the nondeterministic Initialization Algorithm given in Section 3.

Remark 2. Observe that no initial place is affected by any step of type (a) or (b).

The properties of the above I.V.I.A. (Instantiated Variant of the Initialization Algorithm) that we need to prove are listed in the following

Lemma 4.1. The following conditions hold during execution of the I.V.I.A..

- (4.1) Each $\bar{\alpha}$ is finite and if α is not initial and $t \in \bar{\alpha}$ then $\text{rank}(t)$ is either finite or exceeds $\omega+1$.
- (4.2) $\bar{\alpha} \cap \bar{\beta} = \emptyset$ for every $\alpha \neq \beta$.
- (4.3) $\bigcup_{\alpha(p_j)=1} \bar{\alpha} \subseteq \text{pow}(\bigcup_{\beta(q_j)=1} \bar{\beta})$ for every 'powerset' clause of the form $p_j = \text{pow}(q_j)$
- (4.4) If s is put for the first time into $\bar{\alpha}$ by a step S of type (a) or (b), and $s \in t \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m)$, then immediately after execution of the step S we have $t \notin \bar{\gamma}$ for every $\gamma \in \Pi$.
- (4.5) If $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \cap \bar{\alpha} \neq \emptyset$ then $\{\alpha_1, \dots, \alpha_\ell\}$ is a P-node and there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$
- (4.6) For each place α , $|\bar{\alpha}| < \rho$ implies $\bar{\alpha} \subseteq \sigma_\alpha$.
- (4.7) If the P-edge $A = \{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ satisfies $|\bar{\alpha}| < \rho$, $\bar{\alpha} \neq \sigma_\alpha$, $\bar{\alpha}_j \neq \emptyset$, for all $j = 1, \dots, \ell$ and $|\bar{\alpha}_j| \geq \rho$ for some j , then $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell \not\subseteq \bigcup_{A \rightarrow \beta} \bar{\beta}$ and

$$|\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}| \geq \rho \cdot n.$$

- (4.8) If no P-edge $A = \{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ satisfies all the conditions $|\bar{\alpha}| < \rho$, $\bar{\alpha} \neq \sigma_\alpha$, $\bar{\alpha}_j \neq \emptyset$ for all $j = 1, \dots, \ell$, and $|\bar{\alpha}_j| \geq \rho$ for some j , but there exists some place γ such that $|\bar{\gamma}| < \rho$ & $\bar{\gamma} \neq \sigma_\gamma$, then there also exists a P-edge $B = \{\beta_1, \dots, \beta_m\} \rightarrow \beta$ with $|\bar{\beta}| < \rho$ & $\bar{\beta} \neq \sigma_\beta$ such that

$$\Delta_B = \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \setminus \bigcup_{B \rightarrow \gamma} \bar{\gamma} \neq \emptyset.$$

Moreover $\Delta_B \subseteq \bigcup_{B \rightarrow \delta} \sigma_\delta$ for each such P-edge $B \rightarrow \beta$.

Proof: We proceed by induction on the number of steps (a), (b) executed. First assume that no step (a) or (b) has been executed but that $\bar{\alpha}$ have been initialized in the manner specified by the algorithm. It is then immediate that (4.1), (4.2), and (4.6) all hold, while (4.4) holds vacuously. The remaining points require a bit more discussion.

Proof that (4.3) holds initially: If $\alpha = \alpha_\emptyset$ then $\bar{\alpha} = \{\emptyset\} \subseteq \text{pow}(s)$ for every set s . Next let $\alpha(p_j) = 1$ and $\alpha \neq \alpha_\emptyset$. Pick some $p \in \sigma_\alpha$ such that $p \neq \emptyset$, and let $B = \{\beta_1, \dots, \beta_m\}$ be the set of all β such that $\sigma_\beta \subseteq Mq_j$ and $\sigma_\beta \cap p \neq \emptyset$. Since $\alpha(p_j) = 1$, we have $p \in \sigma_\alpha \subseteq Mp_j = \text{pow}(Mq_j)$, i.e. $p \subseteq Mq_j$; hence $p = \bigcup_{\beta \in B} (\sigma_\beta \cap p)$. Thus for any other powerset clause $p_1 = \text{pow}(q_1)$ we have

$$\begin{aligned} \alpha(p_1) = 1 &\Leftrightarrow p \in Mp_1 \Leftrightarrow p \subseteq Mq_1 \Leftrightarrow \sigma_{\beta_j} \cap p \subseteq Mq_1 \text{ for all } j = 1, \dots, m \\ &\Leftrightarrow \beta_j(q_1) = 1 \text{ for all } j = 1, \dots, m, \end{aligned}$$

proving that $\{\beta_1, \dots, \beta_m\} \rightarrow \alpha$ is a P-edge. Thus α is not initial, from which it follows that $\bar{\alpha} = \emptyset$ initially, so again $\bar{\alpha} \subseteq \text{pow}(s)$ for every set s .

Proof that (4.5) holds initially: Suppose that $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \cap \bar{\alpha} \neq \emptyset$, and let $s \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \cap \bar{\alpha}$, so that $s \subseteq \bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell$ is nonempty. Plainly this s , which belongs to $\bar{\alpha}$ must be an individual, but then $s \subseteq \bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell$ implies that the member ω of s must belong to some $\bar{\alpha}_j$, which is impossible by (4.1). Thus (4.5) is satisfied vacuously.

Proof that (4.7) holds initially: Let $A = \{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ be such that $|\bar{\alpha}| < \rho$, $\bar{\alpha} \neq \sigma_\alpha$, $\bar{\alpha}_j \neq \emptyset$ for $j = 1, \dots, \ell$, and for some α_j ,

$|\bar{\alpha}_j| \geq \rho$. Since initially $\bigcup_{A \rightarrow \beta} \bar{\beta} = \emptyset$, it follows that $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell \not\subseteq \bigcup_{A \rightarrow \beta} \bar{\beta}$. Moreover since $\bar{\alpha}_1, \dots, \bar{\alpha}_\ell$ are all nonempty, since some $|\bar{\alpha}_1| \geq \rho$, and since $2^{\rho-1} \geq 2^{\rho-1} \geq \rho \cdot n$ by the way we have chosen ρ (see the paragraph immediately following the statement of condition (C6) in the preceding section) we have

$$|\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)| > \rho \cdot n.$$

Proof that (4.8) holds initially: Assume that no P-edge $A = \{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ satisfies all the conditions: $|\bar{\alpha}| < \rho$, $\bar{\alpha} \neq \sigma_\alpha$, $\bar{\alpha}_j \neq \emptyset$ for all $j = 1, \dots, \ell$, and $|\bar{\alpha}_j| \geq \rho$ for some j , but there exists some place γ such that $|\bar{\gamma}| < \rho$ & $\bar{\gamma} \neq \sigma_\gamma$. Since $\bar{\alpha}_\emptyset = \sigma_{\alpha_\emptyset}$, and $|\bar{\alpha}| = \rho$ for all other initial places, the last assumption above implies that γ is a non-initial place. Let $t \in \sigma_\beta$ be a set of minimal rank among all sets $s \in \sigma_\gamma$ with γ a non-initial place. Clearly $t \neq \emptyset$, since $\beta \neq \alpha_\emptyset$ because $\alpha_\emptyset$ is an initial place by (C3). Moreover since β is not an initial place, $\sigma_\beta \subseteq \text{Mp}_j$, for some $j \in \{1, \dots, k\}$. Therefore $t \subseteq \text{Mq}_j$. Let $\{\beta_1, \dots, \beta_m\}$ be the set of all places β' such that $\sigma_{\beta'} \cap t \neq \emptyset$. Clearly $\beta_i(q_j) = 1$ for all $i = 1, \dots, m$, and therefore $B = \{\beta_1, \dots, \beta_m\}$ is a P-node. It follows by the remark following Lemma 3.2 of the preceding section that $\{\beta_1, \dots, \beta_m\} \rightarrow \beta$ is a P-edge. By the minimality of rank of t all places β_i are initial, since otherwise there would exist some $t' \in t \cap \sigma_{\beta_i}$ where β_i was non-initial, and then plainly t' would have lower rank than t . Since by our assumption $|\beta_i| < \rho$ for all $i = 1, \dots, m$, it follows that $m = 1$ and $\beta_1 = \alpha_\emptyset$. Therefore $\Delta_B = \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \setminus \bigcup_{B \rightarrow \delta} \bar{\delta} = \text{pow}^*(\alpha_\emptyset) = \{\{\emptyset\}\} \neq \emptyset$, and moreover $\Delta_B = \text{pow}^*(\alpha_\emptyset) \subseteq \sigma_\beta \subseteq \bigcup_{B \rightarrow \delta} \sigma_\delta$, which proves (4.8).

This completes our first induction step. Next we assume that (4.1)-(4.8) all hold immediately before a step S of type (a) or (b) is

executed and show that all these statements must still hold after execution of this step.

Proof of (4.1): All elements initially placed in any set $\bar{\alpha}$ are either of finite rank (namely the $\emptyset$ in $\alpha_{\emptyset} = \{\emptyset\}$) or are individuals of rank $\omega+1$ and all $\bar{\alpha}$ are initially finite. If all the elements of a finite set s are either of finite rank or of rank at least $\omega+1$, then every subset of s , i.e. element of $\text{pow}(s)$, is plainly either of finite rank or of rank at least $\omega+2$. The set $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_2)$ is a subset of $\text{pow}(\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_2)$, and in all steps s of either kind (a), (b) all elements added to any set $\bar{\alpha}$ belong to $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_2)$. It follows by induction that $\bar{\alpha}$ remains finite after execution of step S , and that if α is not initial and $t \in \bar{\alpha}$ then $\text{rank}(t)$ is either finite or greater than $\omega+1$.

Proof of (4.2): Let $\alpha \neq \beta$ and let $\bar{\alpha}'$, $\bar{\beta}'$ be the new values which the sets $\bar{\alpha}$, $\bar{\beta}$ take on immediately after step S is executed. We distinguish four cases:

Case (a): If $\bar{\alpha}' = \bar{\alpha}$, $\bar{\beta}' = \bar{\beta}$ then $\bar{\alpha}' \cap \bar{\beta}' = \emptyset$ by induction hypothesis.

Case (b): If $\bar{\alpha}' \neq \bar{\alpha}$, $\bar{\beta}' \neq \bar{\beta}$ then $\bar{\alpha}' = \bar{\alpha} \cup t_1$, $\bar{\beta}' = \bar{\beta} \cup t_2$ where $t_1 \neq \emptyset$ and $t_2 \neq \emptyset$. If step S is of type (a), then $t_1, t_2 \subseteq \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_2) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}$ for some $A = \{\alpha_1, \dots, \alpha_2\}$ such that $A \rightarrow \alpha$, $A \rightarrow \beta$ are P -edges, and $t_1 \cap t_2 = \emptyset$. The same conclusion follows easily even if step S is of type (b), since in this case $t_1 \subseteq \sigma_{\alpha}$, $t_2 \subseteq \sigma_{\beta}$, and $\sigma_{\alpha} \cap \sigma_{\beta} = \emptyset$.

Therefore $(t_1 \cup t_2) \cap (\bar{\alpha} \cup \bar{\beta}) = \emptyset$ in all these cases. Since by induction hypothesis $\bar{\alpha} \cap \bar{\beta} = \emptyset$ it is clear that we still have $\bar{\alpha}' \cap \bar{\beta}' = \emptyset$ after step S is executed.

Case (c): If $\bar{\alpha}' \neq \bar{\alpha}$, $\bar{\beta}' = \bar{\beta}$ then $\bar{\alpha}' = \bar{\alpha} \cup t$ for some $t \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \setminus \bigcup_{A \rightarrow \gamma} \bar{\gamma}$ where $A = \{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ is a P-edge. It follows by induction hypotheses (4.2) and (4.5) that $\bar{\alpha}' \cap \bar{\beta}' = \emptyset$.

Case (d): The case $\bar{\alpha}' = \bar{\alpha}$, $\bar{\beta}' \neq \bar{\beta}$ is symmetric to the preceding case.

Proof of (4.3): If no set $\bar{\alpha}$ for which $\alpha(p_j) = 1$ is modified by step S then

$$\alpha(p_j) \cup \bar{\alpha}' = \alpha(p_j) \cup \bar{\alpha} \subseteq \text{pow}(\bigcup_{\beta(q_j)=1} \bar{\beta}) \subseteq \text{pow}(\bigcup_{\beta(q_j)=1} \bar{\beta}'),$$

by induction hypothesis, where as before $\bar{\alpha}'$, $\bar{\beta}'$ indicate the values assumed by the sets $\bar{\alpha}$, $\bar{\beta}$ immediately after step S is executed. On the other hand if $\alpha(p_j) = 1$ and s is put into $\bar{\alpha}$ by step S then $s \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$ for some P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ by definition of the I.V.I.A., irrespective of whether S is of type (a) or (b). But then $\alpha_1(q_j) = \dots = \alpha_\ell(q_j) = 1$ by Definition 3.1, which implies $s \in \text{pow}(\bigcup_{\beta(q_j)=1} \bar{\beta}')$, showing that (4.3) continues to hold immediately after step S.

Proof of (4.4): Assume that s is put into $\bar{\alpha}$ for the first time during execution of step S and let t be such that $s \in t \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m)$. If $t \in \bar{\gamma}$ for some place γ then since $\text{rank}(t) \neq \omega+1$ (cf. (4.1)), γ is not initial. It follows that t must have been put into $\bar{\gamma}$ in some preceding step S_0 of type (a) or (b) for some P-edge $\{\gamma_1, \dots, \gamma_\ell\} \rightarrow \gamma$. Hence $t \in \text{pow}^*(\bar{\gamma}_1, \dots, \bar{\gamma}_\ell)$ which implies that we must have had $s \in \bar{\gamma}_j$ for some j immediately prior to the execution of step S_0 . But this is impossible by (4.2) since s is an element newly introduced into the set $\bar{\alpha}$.

Proof of (4.5): Assume that $\text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell') \cap \bar{\alpha}' \neq \emptyset$ immediately after step S is executed, where as previously $\bar{\alpha}_j$ designates the value assumed by $\bar{\alpha}_j$ immediately after step S. If $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \cap \bar{\alpha} \neq \emptyset$ before step S, then by induction hypothesis $\{\alpha_1, \dots, \alpha_\ell\}$ is a P-node and there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$. On the other hand if $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \cap \bar{\alpha} = \emptyset$ immediately before step S, then S itself must introduce some new element t into $\text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell') \cap \bar{\alpha}'$. If $t \notin \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$ before step S is executed, then since $t \in \text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell')$ after step S is executed, some new element $s \in t$ must have been introduced into some $\bar{\alpha}_i$ by step S, giving $s \in t \in \text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell')$. Hence it follows by (4.4) that $t \notin \bar{\gamma}'$ for all places γ . This contradicts $t \in \bar{\alpha}'$, thus $t \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$ even before step S is executed. Therefore t must be introduced into $\bar{\alpha}$ by step S, which implies that $t \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m)$ for some $B = \{\beta_1, \dots, \beta_m\}$ for which there exists a P-edge $B \rightarrow \alpha$. It follows by (4.2) and Lemma 3.2 that $\{\beta_1, \dots, \beta_m\} = \{\alpha_1, \dots, \alpha_\ell\}$, which implies that $\{\alpha_1, \dots, \alpha_\ell\}$ is a P-node and there exists a P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$.

Proof of (4.6): Let $|\bar{\alpha}'| < \rho$, where as before $\bar{\alpha}'$ designates the value of $\bar{\alpha}$ immediately after execution of step S. If $\bar{\alpha}' = \bar{\alpha}$ then $\bar{\alpha}' \subseteq \sigma_\alpha$ by induction hypothesis. Otherwise since $|\bar{\alpha}'| < \rho$ step S must be of type (b) and thus $\bar{\alpha}' = \bar{\alpha} \cup t$ with $t \subseteq \sigma_\alpha$ by definition of step (b) of the I.V.I.A.. Thus $\bar{\alpha}' \subseteq \sigma_\alpha$ still holds after step S is executed.

Proof of (4.7): Let $A = \{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ be a P-edge satisfying all the conditions $|\bar{\alpha}| < \rho$, $\bar{\alpha} \not\subseteq \sigma_\alpha$, $\bar{\alpha}_j \neq \emptyset$ for all $j = 1, \dots, \ell$, and $|\bar{\alpha}_j| \geq \rho$ for some j . We distinguish two principal cases.

Case (1): If the P-edge $A \rightarrow \alpha$ satisfies the above conditions immediately before step S is executed then:

Case (1a): Suppose that no $\bar{\beta}$ for which β is a target of A is modified by step S. In this case it follows by induction that

$$|\text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell') \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}'| \geq |\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}| \geq \rho \cdot n$$

(where as above $\bar{\alpha}_1', \dots, \bar{\alpha}_\ell'$ indicate the values assumed by the sets $\bar{\alpha}_1, \dots, \bar{\alpha}_\ell$ immediately after execution of step S). Moreover by induction hypothesis $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell \not\subseteq \bigcup_{A \rightarrow \beta} \bar{\beta}' = \bigcup_{A \rightarrow \beta} \bar{\beta}$. If none of the $\bar{\alpha}_j$ are modified by step S, then (4.7) follows immediately. On the other hand if one of the $\bar{\alpha}_1, \dots, \bar{\alpha}_\ell$ is modified by step S then by (4.4) we have $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' \not\subseteq \bigcup_{A \rightarrow \beta} \bar{\beta}'$, so that (4.7) is true in this case also.

Case (1b): Next suppose that some $\bar{\gamma}$ for which γ is a target of A is modified by step S. We will prove that $(\bar{\gamma}' \setminus \bar{\gamma}) \cap \text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell') = \emptyset$, where $\bar{\gamma}', \bar{\alpha}_1', \dots, \bar{\alpha}_\ell'$ are the new values of $\bar{\gamma}, \bar{\alpha}_1, \dots, \bar{\alpha}_\ell$ after execution of step S. To show this, we proceed by contradiction, and suppose that there exists some element z such that $z \in (\bar{\gamma}' \setminus \bar{\gamma}) \cap \text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell')$. Then by definition of the I.V.I.A., $z \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m)$ for some P-edge $\{\beta_1, \dots, \beta_m\} \rightarrow \gamma$. Hence by (4.2) and Lemma 3.2 we have $A = \{\alpha_1, \dots, \alpha_\ell\} = \{\beta_1, \dots, \beta_m\}$. It follows by the principal hypothesis of (4.7) that S must be a step of type (a). Therefore, after step S, we must have $|\bar{\beta}| \geq \rho$ for every target β of A, contradicting the existence of a P-edge $A \rightarrow \alpha$ satisfying the condition of step (a), i.e. the principal hypothesis of (4.7). This shows that if $z \in \bar{\gamma}' \setminus \bar{\gamma}$ then $z \notin \text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell')$, as claimed. Therefore it follows by induction that

$$|\text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell') \setminus \bigcup_{A \rightarrow \gamma} \bar{\gamma}'| \geq |\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell) \setminus \bigcup_{A \rightarrow \gamma} \bar{\gamma}| \geq \rho \cdot n$$

Next we must prove that $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' \notin \bigcup_{A \rightarrow \beta} \bar{\beta}'$ holds in case (1b), which we do as follows. First suppose that $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' = \bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell$, i.e. that step S modifies no set $\bar{\alpha}_i$. Then by induction hypothesis $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' = \bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_\ell \notin \bigcup_{A \rightarrow \beta} \bar{\beta}$. Therefore if $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' \in \bigcup_{A \rightarrow \beta} \bar{\beta}'$ we must have $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' \in \bar{\beta}_0' \setminus \bar{\beta}_0$ for some target β_0 of A. Since by hypothesis of case (1) all the conditions $|\bar{\alpha}| < \rho$, $\bar{\alpha} \neq \sigma_\alpha$, $\bar{\alpha}_j \neq \emptyset$ for all j, and $|\bar{\alpha}_j| \geq \rho$ for some j, are satisfied by the P-edge $A = \{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ just before step S is executed, step S must be of type (a). Moreover since the P-edge $A \rightarrow \alpha$ satisfies the same conditions above after step S is executed, it follows that step S must be a step of type (a) relative to a P-node $\{\beta_1, \dots, \beta_m\} \neq \{\alpha_1, \dots, \alpha_\ell\}$ having β_0 as one of its targets. But then $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \cap \text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell')$ which by (4.2) and Lemma 3.2 implies $\{\beta_1, \dots, \beta_m\} = \{\alpha_1, \dots, \alpha_\ell\}$, a contradiction. This shows that $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' \notin \bigcup_{A \rightarrow \beta} \bar{\beta}'$ in the case in which step S modifies no set $\bar{\alpha}_i$.

The one remaining subcase of principal case (1) is that in which one of the sets $\bar{\alpha}_i$ is modified by step S. But in this case it follows easily by (4.4) that $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' \notin \bigcup_{A \rightarrow \beta} \bar{\beta}'$.

Having now completed our analysis of principal case (1) of the proof of (4.7), we turn immediately to

Case (2): Here we suppose that the P-edge $A \rightarrow \alpha$ did not satisfy all the conditions $|\bar{\alpha}| < \rho$, $\bar{\alpha} \neq \sigma_\alpha$, $\bar{\alpha}_j \neq \emptyset$ for all j, and $|\bar{\alpha}_j| \geq \rho$ for some j immediately before step S was executed, even though these conditions are satisfied immediately after step S is executed. Since

by (4.6) we have $\bar{\alpha}' \subseteq \sigma_\alpha$ and since $\bar{\alpha}' \neq \sigma_\alpha$ by hypothesis of (4.7), the conditions $|\bar{\alpha}| < \rho$ and $\bar{\alpha} \neq \sigma_\alpha$ must have been satisfied before S was executed. From this it is clear that some new element z must have been put into some one of the $\bar{\alpha}_i$ by step S. Moreover there must be some α_j such that $|\bar{\alpha}_j| \geq \rho$. If $i \neq j$ then there clearly exist $2^{\rho-1}$ elements of $\text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_\ell)$ having the form $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_{j-1}' \cup \bar{\alpha}_{j+1}' \cup \dots \cup \bar{\alpha}_\ell' \cup s$, where $s \subseteq \bar{\alpha}_j'$ and $s \neq \emptyset$. Clearly all these sets contain z as an element, and since z was put into $\bar{\alpha}$ for the first time by step S, it follows by (4.4) that none of these sets belongs to $\bigcup_{A \rightarrow \beta} \bar{\beta}'$. This shows that

$$|\text{pow}^*(\bar{\alpha}_1', \dots, \bar{\alpha}_\ell') \setminus \bigcup_{A \rightarrow \beta} \bar{\beta}'| \geq 2^{\rho-1} \geq 2^{\rho-1} \geq \rho \cdot n.$$

Next we show that the same assertion follows even if $i = j$. Indeed, in this case we can reason in just the same way, except that now the number of sets of the form $\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_{i-1}' \cup \bar{\alpha}_{i+1}' \cup \dots \cup \bar{\alpha}_\ell' \cup s$ with $z \in s \subseteq \bar{\alpha}_i'$ that do not belong to $\bigcup_{A \rightarrow \beta} \bar{\beta}'$ can only be asserted to be at least $2^{\rho-1}$ (however, this is all we need). Finally since $z \in \bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell'$ and z is newly inserted into $\bar{\alpha}_i'$ by step S we have

$$\bar{\alpha}_1' \cup \dots \cup \bar{\alpha}_\ell' \notin \bigcup_{A \rightarrow \beta} \bar{\beta}'.$$

by (4.4), completing the proof of (4.7).

Proof of (4.8): Assume that no P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ satisfies the conditions $|\bar{\alpha}| < \rho$, $\bar{\alpha} \neq \sigma_\alpha$, $\bar{\alpha}_i \neq \emptyset$ for all $i = 1, \dots, \ell$, and $|\bar{\alpha}_i| \geq \rho$ for some i , but there is some α such that $|\bar{\alpha}| < \rho$ & $\bar{\alpha} \neq \sigma_\alpha$. Let $t \in \sigma_\beta \setminus \bar{\beta}$ be a set of minimal rank among all sets $s \in \sigma_\gamma \setminus \bar{\gamma}$, $|\bar{\gamma}| < \rho$.

CLAIM: $t \in \Delta_B = \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \setminus \bigcup_{B \rightarrow \delta} \bar{\delta}$ for some P-node $B = \{\beta_1, \dots, \beta_m\}$.

Indeed, β is not initial because $|\bar{\beta}| < \rho$ and $\beta \neq \alpha_\emptyset$ since $\bar{\alpha}_\emptyset = \sigma_{\alpha_\emptyset} = \{\emptyset\}$. Thus β is the target of some edge, and thus it follows from Definition 3.1 that $\sigma_\beta \subseteq \text{Mp}_j$ for some j . Let $\beta_1, \dots, \beta_m$ be all places β' such that $\sigma_{\beta'} \cap t \neq \emptyset$. Since $t \subseteq \text{Mq}_j$, we have $\beta_i(q_j) = 1$ for all $i = 1, \dots, m$, which shows that $B = \{\beta_1, \dots, \beta_m\}$ is a P-node. The Remark immediately following Lemma 3.2 shows that $\{\beta_1, \dots, \beta_m\} \rightarrow \beta$ is a P-edge. If $t \cap \bar{\beta}_1 = \emptyset$, then any $t' \in \sigma_{\beta_1} \cap t$ would have rank smaller than t and would belong to $\sigma_{\beta_1} \setminus \bar{\beta}_1$; hence the minimality of $\text{rank}(t)$ implies that $\bar{\beta}_1 \neq \emptyset$, for all $i = 1, \dots, m$. Therefore, since no P-edge $\{\alpha_1, \dots, \alpha_\ell\} \rightarrow \alpha$ satisfies the conditions enumerated above, it follows that $|\bar{\beta}_i| < \rho$ for all $i = 1, \dots, m$, which by (4.6) implies $\bar{\beta}_i \subseteq \sigma_{\beta_i}$, $i = 1, \dots, m$. We noted just above that $t \cap \bar{\beta}_1 \neq \emptyset$ follows from the minimality of $\text{rank}(t)$, so that $t \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m)$.

To prove that $\text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \setminus \bigcup_{\{\beta_1, \dots, \beta_m\} \rightarrow \gamma} \bar{\gamma} \neq \emptyset$, we will now show that $t \notin \bigcup_{B \rightarrow \beta} \bar{\gamma}$, where $B = \{\beta_1, \dots, \beta_m\}$. We proceed by contradiction, i.e. assume that $t \in \bigcup_{B \rightarrow \gamma} \bar{\gamma}$, and let γ_0 be the target of B for which $t \in \bar{\gamma}_0$. Since γ_0 is not initial, it follows that t must have been introduced into $\bar{\gamma}_0$ by some earlier step S_0 of type (a) or (b) relative to a P-node $\{\gamma_1, \dots, \gamma_r\}$ having γ_0 as one of its targets. But then $t \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \cap \text{pow}^*(\bar{\gamma}_1, \dots, \bar{\gamma}_r)$, so that by (4.2) and Lemma 3.2 $\{\gamma_1, \dots, \gamma_r\} = \{\beta_1, \dots, \beta_m\}$. Since $|\bar{\beta}_1| < \rho$ for all $i = 1, \dots, m$, this implies that step S_0 must be of type (b). Inspection of the code of step (b) of the I.V.I.A. shows that since $t \in \sigma_\beta$, the set $\bar{\gamma}_0$ into which S_0 introduces t must be $\bar{\beta}$, contradicting the fact

that $t \in \sigma_\beta \setminus \bar{\beta}$. This contradiction shows that $t \notin \bigcup_{\beta \rightarrow \gamma} \bar{\gamma}$, verifying that $\Delta_\beta = \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \setminus \bigcup_{\beta \rightarrow \gamma} \bar{\gamma} \neq \emptyset$, as claimed.

It only remains to show that $\Delta_\beta \subseteq \bigcup_{\beta \rightarrow \gamma} \sigma_\gamma$. To see this, let $s \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \subseteq \text{pow}^*(\sigma_{\beta_1}, \dots, \sigma_{\beta_m})$. Since $\sigma_{\beta_1} \cup \dots \cup \sigma_{\beta_m} \subseteq \text{Mq}_j$, we have $s \in \text{pow}(\text{Mq}_j) = \text{Mp}_j$. Let γ be the place such that $s \in \sigma_\gamma$. Then $\text{pow}^*(\sigma_{\beta_1}, \dots, \sigma_{\beta_m}) \cap \sigma_\gamma \neq \emptyset$, from which it follows by the Remark just after Lemma 3.2 that $\{\beta_1, \dots, \beta_m\} \rightarrow \gamma$ is a P-edge. This proves that $\Delta_\beta \subseteq \bigcup_{\beta \rightarrow \gamma} \sigma_\gamma$ completing the proof of property (4.8) and hence that of Lemma 4.1. Q.E.D.

To prove that the number of successive steps of the I.V.I.A. executed before it terminates is at most $n 2^n$, note that in the I.V.I.A. each set node $B = \{\beta_1, \dots, \beta_m\}$ is processed at most once by step (a), since after B has been processed every target α of B satisfies $|\bar{\alpha}| \geq \rho$. On the other hand it follows by inspection of step (b) and from the final conclusion of (4.8) that immediately after $\{\beta_1, \dots, \beta_m\}$ is processed by a step S of type (b) we must have $\text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m) \subseteq \{\beta_1, \dots, \beta_m\} \rightarrow \bar{\beta}'$ (where as above symbols $\bar{\beta}_j$ designate values just before S and $\bar{\beta}'$ values just after S), so that step (b) will not again be applied to the P-node $\{\beta_1, \dots, \beta_m\}$ until some new element has been added to at least one of the sets $\bar{\beta}_1, \dots, \bar{\beta}_m$. It follows that by the $(\rho-1) \cdot m$ -th time $\{\beta_1, \dots, \beta_m\}$ has processed in step (b) each $\bar{\beta}_j$ must have at least $(\rho-1)$ elements. Thus the P-node $\{\beta_1, \dots, \beta_m\}$ can be processed at most ρn times by the I.V.I.A. Since there are no more than 2^n set nodes, it follows that the total number of steps (a), (b) which the I.V.I.A. can execute before halting is bounded by $\rho n 2^n$.

It is now easy to complete the proof that condition (C6) holds

upon termination of the I.V.I.A. For this, note first of all that properties (C6b,c,d) are the same as (4.2), (4.3) and (4.5). Because of (4.1), to prove (C6a) we need only show that upon termination of our instantiated version of the Initialization Algorithm no set $\bar{\alpha}$ is empty. But this is clear since when the computation stops there is no place α such that $|\bar{\alpha}| < \rho$ and $\bar{\alpha} \neq \sigma_{\alpha}$ and in particular there is no place α such that $\bar{\alpha} = \emptyset$.

To prove (C6e) we proceed as follows. By (4.1) α is not initial if $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_l \in \bar{\alpha}$, so that in this case $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_l$ must have been put into $\bar{\alpha}$ by some step of type (a) or (b). Thus we must have $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_l \in \text{pow}^*(\bar{\beta}_1, \dots, \bar{\beta}_m)$ for some P-edge $B = \{\beta_1, \dots, \beta_m\} \rightarrow \alpha$, and by Lemma 3.2 and (4.2) this implies $B = \{\alpha_1, \dots, \alpha_l\}$ which shows that $\{\alpha_1, \dots, \alpha_l\}$ is a P-node. Observe that since $\bar{\alpha}_1, \dots, \bar{\alpha}_l$ are the values which these sets assume at the end of execution of the I.V.I.A., the step S which puts $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_l$ into $\bar{\alpha}$ is the last step in which the P-node B is processed by the I.V.I.A. Indeed once P-node B is processed by a step of type (a) then by (a1) of the I.V.I.A. $|\bar{\beta}| \geq \rho$ for every target β of B, so that B will never be processed any more. Also by condition (4.8) (see especially its final assertion) a P-node $B = \{\beta_1, \dots, \beta_m\}$ can be processed by a step of type (b) only in the case that either B has never been processed or that some $\bar{\beta}_1$ has been enlarged since the last time the P-node B has been processed.

In order to show that the P-edge $\{\alpha_1, \dots, \alpha_l\} \rightarrow \alpha$ is marked we first note that if the step S which puts $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_l$ into $\bar{\alpha}$ is of type (a), it follows at once by (a2) of the I.V.I.A. that the P-edge $\{\alpha_1, \dots, \alpha_l\} \rightarrow \alpha$ is marked. Next consider the other possible case, in which step S is of type (b), so that by definition (see the text of the

I.V.I.A.) we have $\bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_l \in \sigma_\alpha$. As remarked above, the P-node $\{\alpha_1, \dots, \alpha_l\}$ is processed for the last time by step S. Therefore $|\bar{\alpha}_i| < \rho$ for all $i = 1, \dots, l$, since otherwise $\{\alpha_1, \dots, \alpha_l\}$ would have been processed by a subsequent step of type (a) before the I.V.I.A. terminated. Moreover, the I.V.I.A. only terminates when there is no place α such that $|\bar{\alpha}| < \rho$ and $\bar{\alpha} \neq \sigma_\alpha$, so that by (4.6) on termination we must have $\bar{\alpha}_i = \sigma_{\alpha_i}$, $i = 1, \dots, l$. Consequently $\sigma_{\alpha_1} \cup \dots \cup \sigma_{\alpha_l} = \bar{\alpha}_1 \cup \dots \cup \bar{\alpha}_l \in \sigma_\alpha$, which shows that the P-edge $\{\alpha_1, \dots, \alpha_l\} \rightarrow \alpha$ is marked (indeed a P-edge $\{\beta_1, \dots, \beta_m\} \rightarrow \beta$ will be marked if and only if $\sigma_{\beta_1} \cup \dots \cup \sigma_{\beta_m} \in \sigma_\beta$; see the proof of Condition (C5)). This completes the proof of (C6e).

Finally, to prove (C6f), let s be a non-empty set whose rank is not $\omega+1$ and which is such that $s \in \bar{\alpha}$ for some place α . Then since all non-empty elements of any initial place have rank $\omega+1$, α is not an initial place. Therefore s must have been put into $\bar{\alpha}$ by some step S of the I.V.I.A. of type (a) or (b). It follows that there exists a P-edge $\{\alpha_1, \dots, \alpha_l\} \rightarrow \alpha$ such that $s \in \text{pow}^*(\bar{\alpha}_1, \dots, \bar{\alpha}_l)$, proving (C6f).

This completes the proof that conditions (C1)-(C6) are necessary are necessary for satisfiability of Q , thereby supplying the last element needed to establish our main result, to wit:

Theorem 4.2. Conditions (C1)-(C6) are necessary and sufficient for satisfiability of the set P of clauses; hence the satisfiability of a set of clauses of this form can be decided algorithmically.

Having now proved this main result we go on immediately to sharpen it by showing that if the clause set P is satisfiable it can be satisfied by a collection of sets whose maximum rank can be bounded in terms of the size of P .

5. MODELS OF P OF FINITE AND BOUNDED RANK

As before let P be a conjunction of clauses of types

$$x = y \cup z, \quad x = y \setminus z, \quad x = \emptyset, \quad x \in y, \quad x \notin y, \quad x = \text{pow}(y),$$

and let $y_1, \dots, y_m$ be the distinct variables occurring in P . Assume that P is satisfiable, and let $\Pi, <, \star, \zeta$ be respectively a set of places of P , an ordering of variables $y_1, \dots, y_m$, and an ordering of places in Π satisfying all the conditions (C1-6) stated in Section 3. We will now show that condition (C6a) can be restated in the following sharpened form:

(C6a') Each $\bar{\alpha}$ is a finite non-empty set and every element of $\bar{\alpha}$ either has a finite rank or a rank greater than ω and less than $(\omega+1)+\lambda$, where $\lambda = 2^{m+2^{m+1}}$.

Indeed by (C6) the sets $\bar{\alpha}$ are constructed in at most $n2^{\Pi\rho}$ executions of step 2 of the Initialization Algorithm, where n is the number of places in Π and ρ is any integer such that $2^{\rho-1}/n \geq \rho$, so that in particular we can take $\rho = 2^n$. Since a place of P is just a boolean function on the set $\{y_1, \dots, y_m\}$, it follows that $n \leq 2^m$, so that $n2^{\Pi\rho} = n2^{2^n} \leq 2^m \cdot 2^{2^{m+1}} = \lambda$, i.e. the number of times that step 2 of the Initialization Algorithm is executed is bounded by λ . Moreover, it is plain that each execution of step 2 can at most augment the rank of a set $\bar{\alpha}$ of maximum rank by 1, from which (C6a') follows immediately since individuals have rank $\omega+1$.

From this we can easily set an upper bound for the rank of all sets appearing in our final model of the clauses P . Indeed, since any step either of type (a) or (b) of the Filling Algorithm increases the

rank of the set $\bar{\alpha}$ of maximum rank by at most 1, and since the Filling Algorithm executes at most $m + m2^n$ steps (because exactly m steps of type (a) are executed, and for each step of type (a) there are at most 2^n stabilization substeps of type (b)), it follows easily that when the Filling Algorithm terminates, each set $\bar{\alpha}$ has rank at most $(\omega+1) + \nu$, where $\nu = 2^{m+1} + 2^{m+1}$. Indeed, $m + m2^n \leq m + m2^{2^m} < m2^{2^{m+1}}$ is elementary, and $m2^{2^{m+1}} \leq 2^{m+2^{m+1}}$ can easily be proved by induction. Thus $(\omega+1) + 2^{m+2^{m+1}} + m + m2^n \leq (\omega+1) + 2 \cdot 2^{m+2^{m+1}} = (\omega+1) + \nu$ is an upper bound for the rank of any set My .

If for any model M of P we call rank of M the rank of the set $My_1 \dots My_m$, then we have proved

Corollary 5.1. P is satisfiable if and only if it has a model of rank at most $(\omega+1) + \nu$, where $\nu = 2^{m+1} + 2^{m+1}$.

By refining the above argument very slightly it is now easy to prove that if our set of clauses P is satisfiable, then it has a model of a finite rank which can be estimated a priori from the size and structure of P . this statement makes the decidability of P obvious (though by no means does it point to a feasible method of computation!). From the theoretical point of view it is interesting to contrast this statement, which tells us that a mixture of boolean and powerset clauses must have a finitary model of it as any model at all, with the observations made in [CFS84] concerning sets of clauses including union clauses $x = Un(y)$ (where $Un(y)$ designates $\{z: (\exists x)(x \in y \ \& \ z \in x)\}$). As noted in that paper, it is easy to write clause sets of this latter (still decidable) form which only have infinite models.

To show that satisfaction of powerset clauses can never require

infinite models, we can simply observe that in the foregoing construction, individuals have been defined to have rank $\omega+1$ just to prevent accidental formation of new 'individuals' in consequence of the execution of a finite number of steps 2 of the Initialization Algorithm and/or step (a) or (b) of the Filling Algorithm; if this happened, disjointness would be disrupted. However, we can obtain the same effect by starting with 'individuals' which are sets of sufficiently large, but nevertheless finite, rank. Specifically, we can use 'individuals' which are doubleton sets of the form $\{\mu, i\}$ where as above $\mu = 2^{m+1} + 2^{m+1}$ and where i is any integer less than μ . Since this allows μ different individuals, all initial places can be initialized in just the manner previously described, since the Initialization Algorithm makes use of at most $p \cdot n = 2^n \cdot n \leq 2^{m+2^m} < \mu$ different individuals. Also, since the total number of steps performed by the Initialization and Filling Algorithms is less than μ , no individual can ever be constructed starting from the empty set, nor can individuals be constructed from other individuals, since any set containing an individual directly or indirectly will have a rank exceeding that of any individual. Thus our proof of necessity and sufficiency of condition (C1-6) for satisfiability can proceed exactly as before, giving

Corollary 5.2. P is satisfiable if and only if it has a model of rank $2^{2^{m+1}+m+2}+1$, where m is the number of variables occurring in P .

Bibliography

- [FOS 80] Ferro, A., Omodeo, E.G., Schwartz, J.T., Decision procedures for elementary sublanguages of set theory, I. Multilevel syllogistic and some extensions, Comm. Pure Appl. Math. XXXIII, 599-608, 1980.
- [BFOS 81] Breban, M., Ferro, A., Omodeo, E.G., Schwartz, J.T., Decision procedures for elementary sublanguages of set theory. II. Formulae involving restricted quantifiers together with ordinal, integer, map and domain notions, Comm. Pure Appl. Math. XXXIV, 2, 1981.
- [BF 84] Breban, M., Ferro, A., Decision procedures for elementary sublanguages of set theory. III. Restricted classes of formulas involving the powerset operator and the general set union operator (to appear in Advances in Appl. Math.).
- [CFMS 84] Cantone, D., Ferro, A., Micale, B., Sorace, G., Decision procedures for elementary sublanguages of set theory. IV. Formulae involving a rank operator and formulae involving one occurrence of the set operator $\Sigma(x) = \{\{y\} | y \in x\}$ (to appear).
- [CFS 84] Cantone, D., Ferro, A., Schwartz, J.T., Decision procedures for elementary sublanguages of set theory. V. Multilevel syllogistic extended by the general union operator (to appear in Journ. Comp. Syst. Sci.).
- [F 84] Ferro, A., A note on the decidability of MLS extended by the powerset operator (to appear in Comm. Pure Appl. Math.).

NYU
COMPSCI
TR-156

c.1

Cantone

Decision procedures for elementary

NYU
COMPSCI
TR-156

c.1

Cantone

Decision procedures for...

DATE

SCH. NO.

LIBRARY

**N.Y.U. Courant Institute of
Mathematical Sciences**

251 Mercer St.

New York, N. Y. 10012